



# Department of Homeland Security Daily Open Source Infrastructure Report for 15 February 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- CNN reports two federal air marshals are facing drug charges after allegedly agreeing to smuggle cocaine supplied by a man who turned out to be a government witness. (See item [11](#))
- The Toronto Star reports the Royal Canadian Mounted Police have announced that a series of raids in Toronto, Windsor, Detroit, and New York City has broken up an international human smuggling ring. (See item [15](#))
- CBS reports for the third time in two months an alleged incident of food tampering was reported at a supermarket in Pennsylvania's Lehigh Valley, when a customer said he found a wire in a hoagie. (See item [21](#))
- US-CERT has released Technical Cyber Security Alert TA06-045A: Microsoft Windows, Windows Media Player, and Internet Explorer vulnerabilities. (See item [33](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *February 14, Associated Press* — **IEA chief says members' oil reserves could offset possible Iranian shutdown.** The head of the International Energy Agency (IEA) said Tuesday, February

14 that its member governments could coordinate a release of strategic oil reserves that would offset a shutdown of Iranian crude output for up to 18 months. Asked whether the agency's efforts could wholly mitigate such a production shortfall, Claude Mandil, executive director of the energy watchdog for the Organization for Economic Cooperation and Development, said "The answer is clearly 'yes'." Western leaders fear Iran's nuclear program is aimed at developing nuclear weapons, though Iran insists it is only intended to generate electricity. "We have four billion barrels in strategic stocks," Mandil said. Even taking account lower estimates, he said, the IEA could keep oil supplies flowing for a year and a half. The Paris-based IEA says its member countries hold 4.1 billion barrels in public and industry stockpiles, of which around 1.4 billion barrels are controlled directly by governments for emergency purposes. Mandil said the IEA's coordinated response to hurricanes that hit the United States last year demonstrated that the agency could act effectively. "There won't be problems with IEA members coming on board," if Iranian production is shut down, Mandil added.

Source: [http://biz.yahoo.com/ap/060214/france\\_oil.html?v=1](http://biz.yahoo.com/ap/060214/france_oil.html?v=1)

2. *February 13, KSL-TV 5 (NV)* — **Incidents at Nevada power substations investigated.** The Joint Terrorism Task Force is looking into a series of mysterious incidents at electrical power facilities in Salt Lake Valley, NV. Two more incidents cropped up overnight in which someone tried to deliberately cripple the power grid. One or more people got inside the substation fence and tried to shut down electrical service over a wide area. This time, they failed. The first intruder alert was Sunday night, February 12. Utah Power security called in deputies to the Valley Center substation. Lt. Chris Bertram, Salt Lake County Sheriff's Office said, "...they advised us they had some people that were in one of their substations manipulating the controls of the substation." Whatever the intruders did, it knocked out power to nearly 4,000 homes and businesses. Lt. Chris Bertram said, "Somebody had actually entered into this secure area. They actually shut down the power grids and left the area." Just after midnight, someone struck again a few blocks west at the Carlisle Substation. A backup system prevented a power outage. Two earlier incidents seem to fit the pattern, at a Taylorsville substation Saturday, February 11, and a Holladay substation Friday, January 27th. Both knocked out electricity for thousands of customers.

Source: <http://www.ksl.com/?nid=148&sid=163045>

3. *February 13, Associated Press* — **Plant's owner acknowledges risk of radiation containment failure.** A radiation barrier built inside the Oyster Creek nuclear plant has a 74 percent chance of failing should the plant's reactor core melt or its fuel be damaged in an accident, owner AmerGen Energy Co. said in a re-licensing application. The steel-and-concrete containment system, which surrounds the reactor and its nuclear fuel, is designed to condense steam and cool the reactor in an emergency. AmerGen Energy Co. said in a risk assessment analysis that the radiation barrier is more likely than not to fail, the Asbury Park Press of Neptune reported. The analysis was part of a 2,400-page license application aimed at keeping the plant open after its current license expires in 2009. That estimate would hold true only "in the highly unlikely event that there is a core damage event," said Peter C. Resler, manager of nuclear communications for Exelon, which owns AmerGen. AmerGen is seeking permission to keep Oyster Creek open for another 20 years. David Lochbaum, director of the Nuclear Safety Project for the environmental organization, the Union of Concerned Scientists, said that if an accident occurs, the containment system isn't likely to work.

Source: <http://www.newsday.com/news/local/wire/newjersey/ny-bc-nj--o>

4. *February 13, U.S. Nuclear Regulatory Commission* — **New security requirements for nuclear plant design, certification, and licensing planned.** U.S. Nuclear Regulatory Commission (NRC) Chairman Nils J. Diaz spoke at a Platts Conference in Washington, DC, on Monday, February 13 regarding new plant design, certification, and licensing. He said that the NRC has three important security rulemakings planned or underway to codify security requirements for power reactors. The first is the rulemaking on the design basis threat for radiological sabotage. The proposed rule is currently out for public comment and a final rule will be issued later this year. The second rulemaking will amend the power reactor security regulations in 10 CFR 73.55, 73.56, 73.57, and Part 73 appendices to align them with the series of orders the Commission issued following September 11, 2001, and to ensure safety–security interface issues are properly considered in plant operations. The Commission intends to finalize this rule as early in calendar year 2007 as possible. Finally, the Commission’s expectations on security design for new reactor licensing activities are to be codified in a third rulemaking by September 2007. The expectation of the Commission is that the lessons learned by the agency and reactor licensees pre– and post–9/11/2001 should be considered by the vendors at the design stage.

Source: <http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2006/s-06-002.html>

5. *February 13, Associated Press* — **Push on for LNG to boost energy supplies.** Since hurricanes Katrina and Rita slammed the Gulf Coast, the region has lost more than 610 billion cubic feet of natural gas production, according to the American Gas Association. Analysts advocate placing aboveground storage tanks along the nation's coasts where energy companies can store imported liquefied natural gas (LNG). The urgency to expand the number of storage terminals domestically has grown, analysts say. More than 40 projects have either been proposed, received federal permits or are under construction, though analysts say the market can probably support no more than 15. Two years ago, an explosion at an LNG plant in Algeria killed 30 people. The worst accident on record happened in 1944, at a Cleveland, Ohio, LNG plant that burned and killed 128 people. Industry analysts and executives estimate that percentage of LNG imports could reach 15 percent of U.S. natural gas by 2012. Economists and company executives say increasing reliance on foreign countries for natural gas may not be as dicey as the dependency on other nations for oil. A gas cartel like the Organization of the Petroleum Exporting Countries isn't likely, said James L. Smith, Southern Methodist University's Cary M. Maguire Chair in Oil & Gas Management.

Source: <http://www.thebostonchannel.com/news/7000579/detail.html?rss=bos&psp=news>

6. *February 13, Reuters* — **Recycling nuke fuel may thwart terrorism: DOE secretary.** The Bush administration's plan to recycle spent nuclear fuel could thwart recruitment efforts by terrorist groups in poor countries by providing impoverished nations with affordable electricity supplies that would improve their economies and the lives of their citizens, U.S. Energy Secretary Sam Bodman said on Monday, February 13. The administration has asked for funds to develop technology for reprocessing the thousands of tons of spent nuclear fuel stored at U.S. nuclear power plants, which could be supplied to countries as fuel for their new power reactors that would generate electricity. Bodman said the nuclear recycling plan could particularly help underdeveloped nations, which have "frequently served as safe havens for terrorists and other

fanatics," such as the Taliban regime in Afghanistan and Osama bin Laden's initial home base in Sudan. "Even if we are able to quickly and resoundingly defeat the terrorist threat we currently face, we will still be confronted with the...poverty that grips so much of the world," Bodman said in a speech to the Platt's nuclear energy conference. He said if these underdeveloped nations are to build thriving economies, they will need access to reliable energy supplies, which could be met with the proposed nuclear fuel recycling program.

Source: [http://news.yahoo.com/s/nm/20060213/us\\_nm/energy\\_nuclear\\_security\\_dc\\_2](http://news.yahoo.com/s/nm/20060213/us_nm/energy_nuclear_security_dc_2)

7. *February 13, KPRC Local 2 (TX)* — **Electricity kills man climbing transformer.** More than 12,000 volts of electricity killed a man who climbed on top of a southwest Houston, TX transformer, authorities told KPRC Local 2 on Monday, February 13. Officers with the Houston Police Department found the man at about 6 p.m. CST on Sunday, February 12, at the CenterPoint Energy substation on Mullens Drive and Jessamine Street. Witnesses said the man got through a barbed wire fence before climbing the tower. The man, whose identity has not been released, had several cuts on his body. Investigators said the man was not a CenterPoint Energy employee and that they are not sure what the man was doing there.

Source: [http://news.yahoo.com/s/kprc/20060213/lo\\_kprc/3264802](http://news.yahoo.com/s/kprc/20060213/lo_kprc/3264802)

8. *February 12, Associated Press* — **Company breaks ground on \$106 million solar plant in Nevada.** An energy company broke ground over the weekend on Nevada Solar One, which it called the largest solar thermal power plant to be built anywhere in the world in 15 years. Solargenix Energy said it formally began construction on the 64-megawatt plant in the Eldorado Valley of Boulder City on Saturday, February 11. The \$106 million solar project on 300 acres is scheduled for completion by March 2007, when the Solargenix will begin selling energy to the Nevada Power Company and Sierra Pacific Power Company. The plant is expected to provide enough power for about 40,000 households. The plant will use some 19,300 solar receivers, which are parabolic mirrors that direct the sun's heat onto tubes to heat a special fluid to 750 degrees. The fluid then transfers heat to a steam generator to produce electricity. The last U.S. solar thermal power plant was completed in Cramer Junction, CA, 15 years ago. Last week, Powered by Renewables Corp. and SunEdison LLC said they plan to build an 18-megawatt photovoltaic plant by the end of the year in Clark County, NV. They plan to eventually supply enough energy to power 36,000 homes.

Source: <http://www.lasvegassun.com/sunbin/stories/text/2006/feb/12/021210753.html>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

9. *February 13, NBC 6 (FL)* — **Ruptured gas line sparks fire at dry cleaners.** A two-alarm fire burned inside Alex's Dry Cleaners in Miami, FL, for more than two hours Monday morning, February 13. Witnesses reported seeing smoke and flames and hearing explosions. Miami-Dade Fire Rescue crews at the scene said they believe a ruptured gas line started the blaze and caused the explosions. No injuries were reported.

Source: <http://www.nbc6.net/news/7008311/detail.html>

[[Return to top](#)]

## **Defense Industrial Base Sector**

Nothing to report.

[[Return to top](#)]

## **Banking and Finance Sector**

10. *February 13, Denver Post* — **Colorado identity theft ring broken.** Thirteen people have been indicted in connection with identity theft, which Jefferson County District Attorney Scott Storey called a "very significant issue in our community." The two grand jury indictments unsealed Friday, February 10 charge 13 individuals — nine in one group and four in another — with violating the Colorado Organized Crime Control Act, possession of a controlled substance, theft, computer crime, possession of methamphetamine, conspiracy to commit theft, and forgery. One indictment contains a total of 96 counts and the other has 60 counts. From January 1, 2004 through January 31, 2005, members of one ring stole mail from mailboxes and created fictional checks and identification documents on a computer. The suspects opened credit accounts, cashed the phony checks, opened bank accounts in false names, and bought items with the money frequently used to buy drugs. Jackson said the second group "operated a little more simply." Group members would "get high on methamphetamines and sit on the phone and call banks" to obtain financial information that they would use to make forged checks, he said. The checks would be cashed or used to buy items at stores and banks with the aim of buying drugs.

Source: [http://www.denverpost.com/ci\\_3505640?source=rss](http://www.denverpost.com/ci_3505640?source=rss)

[[Return to top](#)]

## **Transportation and Border Security Sector**

11. *February 14, CNN* — **Air marshals face smuggling charges.** Two federal air marshals are facing drug charges after allegedly agreeing to smuggle cocaine supplied from a man who turned out to be a government witness, the U.S. attorney's office in Houston, TX, announced Monday, February 13. Shawn Ray Nguyen, 38, and Burlie Sholar, 32, were arrested Thursday, February 9, after allegedly receiving 15 kilograms of cocaine and \$15,000 cash delivered to Nguyen's home and agreeing to take the drugs on a plane, prosecutors said in court papers. The U.S. attorney's office accused the two men of agreeing to use their official positions as federal air marshals to bypass airport security and smuggle the cocaine on board a flight from Houston to Las Vegas, NV, in exchange for the money. The two men made an initial appearance in federal court Monday and will have a detention hearing before Thursday, February 16, where bail will be discussed. "The alleged conduct of these two men is serious and disturbing," the inspector general for the Department of Homeland Security, Richard Skinner, said. Upon conviction, the charge of conspiracy to possess with intent to distribute five kilograms or more of cocaine carries a mandatory minimum prison sentence of 10 years and a maximum of life.
- Source: <http://www.cnn.com/2006/LAW/02/13/marshals.cocaine/index.html>

12. *February 14, Government Accountability Office* — **GAO-06-296: Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be**



**Implemented (Report).** Security (DHS) has established a program—the U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT)—to collect, maintain, and share information, including biometric identifiers, on selected foreign nationals entering and exiting the United States. US–VISIT uses these identifiers (digital finger scans and photographs) to screen persons against watch lists and to verify that a visitor is the person who was issued a visa or other travel document. Visitors are also to confirm their departure by having their visas or passports scanned and undergoing finger scanning at selected air and sea ports of entry (POE). The Government Accountability Office (GAO) has made many recommendations to improve the program, all of which DHS has agreed to implement. GAO was asked to report on DHS’s progress in responding to 18 of these recommendations. GAO is closing its existing recommendation related to DHS’s assessment of Increment 2B and recommending that DHS explore alternative means to fully assess the impact of US–VISIT entry capabilities on land POEs. In its comments on a draft of this report, DHS stated that it agreed with many areas of the report and disagreed with others. It also concurred with the need to quickly implement GAO’s open recommendations.

Highlights: <http://www.gao.gov/highlights/d06296high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-296>

13. *February 14, Associated Press* — **Man jumped from Delta flight in Atlanta.** A man is hospitalized in fair condition after authorities say he jumped from a door of a Delta flight that had just landed in Atlanta on Tuesday, February 14. The plane from Orlando, FL, landed at the Atlanta airport about 8:30 a.m. EST. The Transportation Security Administration's Christopher White said the man opened the catering door of the plane and jumped to the tarmac, 30 feet below. White says the man had complained of feeling ill during the flight.  
Source: [http://www.wfaa.com/sharedcontent/dws/wfaa/latestnews/stories/wfaa060214\\_lj\\_delta.2848bca4.html](http://www.wfaa.com/sharedcontent/dws/wfaa/latestnews/stories/wfaa060214_lj_delta.2848bca4.html)
14. *February 14, Associated Press* — **Rhode Island to expand Boston commuter rail in South County.** Two new commuter rail stations proposed by Rhode Island officials could connect Boston to communities south of Providence as early as 2008. The first station will be built near T.F. Green Airport in Warwick, RI, followed by a second station in North Kingstown, RI, Department of Transportation Director James Capaldi said. This marks the first expansion of rail service since 1988, when Massachusetts Bay Transportation Authority trains returned to Providence after a seven-year break. The \$225 million project, financed mostly by state and federal money, would give commuters an attractive alternative to the increasingly congested highways and boost the area's economic growth, state officials said. The Warwick station would connect drivers and rail and air passengers, Capaldi said. Plans include a 1,300-foot skywalk linking the station to the airport. Fees paid by people renting cars from companies located at the station's new five-story garage would pay for part of the project and maintenance  
Source: <http://www.ecnnews.com/cgi-bin/05/snstory.pl?-sec-News+1k589gO+fn-ma.commuterrail.0214-20060214->
15. *February 14, Toronto Star (Canada)* — **Cross-border sting cracks people smugglers.** A series of early morning raids in Toronto, Windsor, Detroit, and New York City has broken up an international human smuggling ring, the Royal Canadian Mounted Police (RCMP) said on Tuesday, February 14. The criminal gang smuggled people from many countries across the Canada–U.S. border, officials said. The two-year investigation was conducted by the RCMP,

the U.S. Department of Homeland Security, Immigration and Customs Enforcement, and the Canada Border Services Agency. Police are alleging that migrants from China, Korea, Albania and Eastern Europe arrived in North America and were then smuggled across the border hidden in trunks of autos, on rail cars, in the backs of transport trucks and on small boats.

Source: [http://www.thestar.com/NASApp/cs/ContentServer?pagename=thesar/Layout/Article\\_Type1&c=Article&pubid=968163964505&cid=1139914922210&col=968705899037&call\\_page=TS\\_World&call\\_pageid=968332188854&call\\_pagepath=News/World](http://www.thestar.com/NASApp/cs/ContentServer?pagename=thesar/Layout/Article_Type1&c=Article&pubid=968163964505&cid=1139914922210&col=968705899037&call_page=TS_World&call_pageid=968332188854&call_pagepath=News/World)

- 16. *February 14, Miami Herald (FL)* — Miami passport lines should speed up.** Miami International Airport (MIA) and U.S. Customs and Border Protection officials have announced a plan to help ease the long lines of international travelers waiting to show their passports to be admitted into the country. The plan, expected to take effect in May, involves building new passport-control booths at Concourse F and using booths in the Concourse E Satellite terminal now reserved for in-transit international passengers. Doing that would nearly double the number of booths available for international travelers entering the country in Miami. Customs and Border Protection now operates 36 booths at Concourse E inside the main terminal, where the bottleneck is occurring. The plan calls for adding between 14 and 18 booths in Concourse F, plus opening 16 more booths in Satellite E that are used for passengers transferring directly to another international flight. The long-lines issue made headlines last summer when the U.S. General Accountability Office released a report saying MIA had the country's worst passport control delays. On average, the GAO report said, MIA passport control officers took about 50 minutes to process a planeload of international travelers, compared to an average of 30 to 40 minutes at other airports around the country.

Source: <http://www.miami.com/mld/miamiherald/13865289.htm>

- 17. *February 09, Salt Lake Tribune (UT)* — More planes show tampering.** Detectives investigating the attempted theft of an airplane at a West Jordan airport Monday night have since found two other planes that were tampered with. Airport spokesperson Barbara Gann said it is likely the incidents are connected. Police were called to the Salt Lake City Municipal Airport No. 2 on Monday night, February 6, when a single engine airplane was found idling near the end of the runway. The aircraft had been cut free of its tether and driven to the place where airport authorities found it unmanned, police said. On Tuesday night, February 7, officers were called to investigate a possible break-in after a pilot reported that the inside of his plane appeared to have been disturbed, Gann said. During the investigation, West Jordan police, airport police and FBI agents found a third plane that appears to have been broken into.

Source: [http://www.sltrib.com/utah/ci\\_3490244](http://www.sltrib.com/utah/ci_3490244)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

18. *February 13, Stop Soybean Rust News* — **Florida finds soybean rust in same Dade County kudzu as last year.** The kudzu site in Dade, FL, that was confirmed with soybean rust on April 29, 2005 was found to have soybean rust sporulating on its still-green leaves last week. In 2005, the April 29 soybean rust find in Dade County (home to Miami in southeast Florida) was the fourth of the season for the state. It was also the first 2005 Florida find south of the nation's first confirmed soybean rust of the year in Pasco, FL, on February 23, 2005. Florida had one county positive for soybean rust post-season in 2004 — Gadsden. Soybean rust was confirmed there in a university test plot in Quincy on November 17. In 2005, Gadsden County was confirmed to have soybean rust on July 17; and this year was one of nine Florida counties with soybean rust announced on January 17. Florida is now reporting 11 counties positive for soybean rust in 2006, bringing the U.S. total to 14 positive counties.  
Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=684>

[[Return to top](#)]

## **Food Sector**

19. *February 14, Associated Press* — **Japanese lawmaker group: U.S. processes beef perfectly.** A group of Japanese lawmakers said Tuesday, February 14, they believe most U.S. companies process beef "perfectly" following an inspection tour of processing plants in Kansas. But the farm minister said Japan will not lower its safety standards for U.S. beef imports because of mad cow fears. The five lawmakers from the ruling Liberal Democratic Party also severely criticized U.S. authorities over a veal shipment last month with banned bone material that prompted Japan to halt U.S. beef imports, saying there would be no resumption without a full investigation. "We got the impression the plants were handling meat bound for Japan perfectly," said Toshikatsu Matsuoka, a former senior farm minister who led a tour to three Kansas facilities. "But it's also true the U.S. authorized an irresponsible company to export beef to Japan, causing trouble for everyone and threatening Japan's food supply," Matsuoka said. "That's unforgivably sloppy, and imports won't be resumed till we get a thorough explanation" from the U.S., he said.  
Source: <http://www.cattlenetwork.com/content.asp?contentid=18466>
20. *February 14, Japan Economic Newswire* — **Japan farm minister opposed to plan to ease beef trade conditions.** Japanese farm minister Shoichi Nakagawa expressed opposition Tuesday, February 14, to a plan by the World Organization for Animal Health (OIE) to ease standard restrictions on beef trade in connection with mad cow disease. The agriculture, forestry and fisheries minister said at a press conference that Japan will try to defend its position as a major importer of beef products. The OIE proposal calls for removing the age limit for cows of 30 months on trade in boneless beef, which would be advantageous for exporters of beef products. As opposition was also expressed by many participants in an expert meeting convened February 7, the government intends to oppose the proposal in an imminent report to the OIE, government officials said. In mid-December, Japan lifted its two-year-old ban on U.S. beef imports that it imposed due to mad cow disease concerns, but it reintroduced the ban on January 20 after a prohibited backbone was found in a shipment of beef from the U.S.  
Source: <http://www.tmcnet.com/usubmit/2006/02/14/1369976.htm>



21. *February 13, CBS 3 (PA)* — **Food tampering incidents continue in Lehigh Valley.** For the third time in two months an alleged incident of food tampering was reported at a supermarket in Pennsylvania's Lehigh Valley. A customer said he found a wire in a hoagie, while at King's Supermarket in Bethlehem Friday, February 10. This case is the latest in a string of food tampering incidents reported to police in the Lehigh Valley over the past month at the same King's Supermarket. Police said pins have reportedly been found in an onion, two packages of ground beef, and a deli ham. A week after those incidents, a man told police that he found a rusty needle in a loaf of bread from a Giant on Easton Avenue in Bethlehem Township. Four days later, officials said another man reported finding a needle in a sealed can of soup bought at another Giant in Northampton County. Police in the Lehigh Valley said it is too early in the investigation to determine when the tampering occurred.

Source: [http://kyw.com/topstories/local\\_story\\_044153807.html](http://kyw.com/topstories/local_story_044153807.html)

22. *February 13, News Channel 5 (OH)* — **Forty-one probable salmonella cases linked to restaurant.** A Woodmere, OH, restaurant remains closed as the board of health investigates several probable cases of salmonella. The Cuyahoga County Board of Health (CCBH) said that 12 confirmed cases and 41 probable cases of salmonella were reported between January 29 and February 10, and officials link the cases to Corky and Lenny's Restaurant. The CCBH provided education and training on food protection to the restaurant staff Monday, February 13, and also submitted samples of restaurant food and food handlers' stool samples to the Ohio Board of Health for analysis. The restaurant closed voluntarily Friday, February 10.

Source: <http://www.newsnet5.com/health/7017624/detail.html>

[[Return to top](#)]

## **Water Sector**

23. *February 14, WROC (NY)* — **Hospital water system tests positive for legionella bacteria.**

The main water system at Strong Memorial Hospital in Rochester, NY, has tested positive for legionella bacteria which can pose a threat to patients with weakened immune systems. The bacteria were found during routine water testing done on February 7th at the hospital.

Currently, one patient is being treated for Legionnaire's Disease at the hospital. Strong is beginning a hyperchlorination of its water system, which flushes higher concentrations of chlorine through the water system to destroy the legionella bacteria. Legionnaire's Disease does not pose a threat to healthy people. However, the disease does affect those with weakened immune systems such as patients undergoing chemotherapy and organ transplants. In patients with compromised immunity, Legionnaire's Disease can cause respiratory problems and/or pneumonia.

Source: <http://www.wroctv.com/news/story.asp?id=21749&r=1>

24. *February 08, U.S. Geological Survey* — **Key challenges for science identified to support Western water management.** Ensuring stable water supplies has grown more complex as the challenges facing water managers continue to mount, especially in the West. Informed decisions of water users and public officials will be necessary to ensure sufficient freshwater resources in the future to support a growing population and economy. The U.S. Geological Survey (USGS) has released a report that examines Western water availability, the modern role

for science, and the value of monitoring and research to ensure an adequate water supply for the Nation's future. According to USGS scientist and coauthor of the report, Mark Anderson, "Effective water management in the West is challenged by increasing and often competing needs among various water users: agricultural use and consumption by cities, maintaining water reservoirs and ensuring in-stream flows for aquatic ecosystems, industrial and energy production, and recreation. Scientific information becomes a crucial factor for resource managers to support their decision-making." Such factors as a demographic shift, climate variability (including the potential for severe sustained droughts), water-rights issues, depletion of ground water in storage, introduction of new storage and water use technologies, and protection of endangered species, add to a growing complexity for water management.

Report: <http://pubs.water.usgs.gov/circ1261/>

Source: <http://www.usgs.gov/newsroom/article.asp?ID=1443>

[[Return to top](#)]

## **Public Health Sector**

**25. *February 14, CBS/Associated press* — Avian flu spreads to Germany, Austria, Iran.** Two dead swans in northern Germany and two birds found dead in Austria appear to have been infected with the virus, health officials in both countries reported Tuesday, February 14. On Tuesday, German Agriculture Minister Horst Seehofer ordered farmers to enclose all poultry and other domestic birds in barns or cages with roofs starting February 20. Authorities determined there was a heightened risk following the discovery of H5N1 in dead swans in Italy and Greece, the first time the highly infectious strain had been detected in the 25-member EU. In Iran, the deadly strain of bird flu has killed 135 wild swans on the Caspian Sea coast, the first such cases detected in the Islamic Republic, the government said Tuesday. Iran's Veterinary Organization said all meat provided under Health Ministry regulations in Iran were free from bird flu and not dangerous to humans, IRNA said.

Source: <http://www.cbsnews.com/stories/2006/02/14/health/main1317986.shtml>

**26. *February 13, BBC News* — Nigeria bird flu screening starts.** Doctors have begun screening workers in northern Nigeria at the first poultry farm to be confirmed with the H5N1 strain of bird flu virus in Africa. The strain was found in birds in three states last week. Thousands of chickens have been dying in Nigeria for more than a month. No humans have tested positive for the virus in Nigeria but there are fears that the emergency measures may have come too late to stop the virus spreading. Mohammed Bala Abubakar, from Kaduna State's health ministry, told the BBC that tests were being carried out on some 120 workers from Sambawa farm in Kaduna State on Monday, February 13, and would continue throughout the week. None of the workers on the farm where the outbreak was first identified have shown any signs of illness, he said. H5N1 has also been found on farms in Kano and Plateau States, on either side of Kaduna. Health ministry officials say there are five other states with suspected bird flu cases: Abuja, where the capital is located, Katsina, Nassarawa, Yobe, and Jigawa states. Experts with protective equipment are being flown in from abroad to help local officials contain the spread of the disease.

Source: <http://news.bbc.co.uk/2/hi/africa/4709890.stm>

27.

*February 13, Associated Press* — **Bird flu vaccine makers to receive protection.** U.S.

Department of Health and Human Services Secretary Mike Leavitt said Monday, February 13, that the administration soon would enter into contracts for bird flu vaccine, rapid tests to detect the virus, and technology that would make the available vaccine go further. "At some point in that process, we'll need to deal with the issue of liability," he told reporters. In December, Congress gave Leavitt the authority to declare when products are necessary "countermeasures" for a public health emergency. The manufacturers and distributors of such products will have liability protections. Under the protections, people injured by a vaccine against bird flu would have to prove willful misconduct to bring a claim for damages. Leavitt said vaccine manufacturers may want the extra protections before conducting clinical trials. "If you're a vaccine manufacturer, you're likely not going to want to move to that step unless you've got adequate liability protection," he said.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/13/AR2006021301494.html>

[\[Return to top\]](#)

## **Government Sector**

28. *February 14, Government Accountability Office* — **GAO-06-403T: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse (Testimony).** As a result of widespread congressional and public interest in the federal response to hurricanes Katrina and Rita, the General Accountability Office (GAO) conducted an audit of the Individuals and Households Program (IHP) under Comptroller General of the United States statutory authority. FEMA provided \$2,000 in IHP payments to affected households via its Expedited Assistance (EA) program. Victims who received EA may qualify for up to \$26,200 in IHP assistance. As of mid-December 2005, IHP payments totaled about \$5.4 billion, with \$2.3 billion provided in the form of EA. These payments were made via checks, electronic fund transfers, and a small number of debit cards. GAO's testimony provides the results to date related to whether (1) controls are in place and operating effectively to limit EA to qualified applicants, (2) indications exist of fraud and abuse in the application for and receipt of EA and other payments, and (3) controls are in place and operating effectively over debit cards to prevent duplicate EA payments and improper usage.

Highlights: <http://www.gao.gov/highlights/d06403thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-403T>

[\[Return to top\]](#)

## **Emergency Services Sector**

29. *February 13, Voice of America* — **Washington, DC-area tests emergency response to train collision.** A recent disaster drill conducted by the Washington, DC, mass transit system — Metro — along with police, firefighters and the Federal Bureau of Investigations, was designed to simulate an explosion and collision of a commuter train and a subway train. According to Chuck Novick of Metro's Safety Department, "The toughest thing for these firefighters and police out here is that they have to work together and we don't want two, three different bosses

up there. We want one person, part of the Unified Command System, that knows what the resources are underneath them and how to utilize those." The exercise tested the response and readiness of Washington, DC–area fire departments and emergency responders and is part of an ongoing effort to strengthen the region's emergency preparedness.

Source: <http://www.voanews.com/english/2006-02-13-voa44.cfm>

30. *February 13, Contra Costa Times (CA)* — **Some California schools tapped as refuge centers in disaster.** San Ramon Valley, CA, schools will become refuge centers as part of an area–wide disaster preparedness plan to help a community fend for itself after an earthquake or a terrorist attack. To that end, the San Ramon Valley Fire District has created a new position dedicated to teach Community Emergency Response Training to school teachers, employees and administrators. In addition, "We're getting amateur radio operators at schools," which would be crucial if cell phone towers are disabled or the system is overwhelmed, said Chris Suter, deputy chief of the San Ramon Valley Fire District. "The amateur radio community is a tremendous asset, an underutilized asset." For the schools, the benefit is immediate, and twofold, explained spokesperson Terry Koehne: If a disaster strikes when young people are in school, then their buildings, the staff and the students will be prepared to ensure they are safe. And the school buildings become disaster hubs for fire, police and other first–responders. Any plan, Koehne said, should be changeable, yet uniform — so firefighters fully understand and know their way around school campuses, and so that the plan remains constant even as school administrators change.

Source: [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/13863868.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/13863868.htm)

31. *February 13, Associated Press* — **Emergency systems in Iowa still have communication gaps.** Millions of dollars have been spent to help Iowa's first responders communicate better in a disaster, but radio problems are still hindering some emergency crews. Almost every one of the state's law enforcement agencies has its own radio frequency, and because some use different systems, they often can't communicate with each other. In many instances, sheriff's departments can't talk directly with police based in the same city. The sheriff's departments in Johnson and Linn Counties have in recent years purchased machines that connect to the systems of other agencies so crews can communicate. "We all realized the inability to talk to each other is a major problem," Coralville police Lt. Ron Wenman said, but he added that it takes 15–30 minutes to deliver the device to an emergency scene. Charlie McClintock, director of the Cedar Rapids Joint Communications Agency, said the best solution would be for eastern Iowa agencies to be dispatched from the same center and be on the same system. But Linn County Sheriff Don Zeller said having all agencies on the same system wouldn't work. If the system broke down, nobody would be able to talk to anyone, Zeller said.

Source: <http://www.siouxcityjournal.com/articles/2006/02/13/news/iowa/af670e5b66065bce8625711400189a3f.txt>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

32. *February 15, SecuriTeam* — **BlackBerry Attachment Service buffer overflow (.doc file).** BlackBerry Enterprise Server software sits behind your organization's firewall and is designed to tightly integrate with existing enterprise systems, securely extending wireless

communications and corporate data to mobile users. Analysis: A corrupt Microsoft Word (.doc) file opened on a BlackBerry wireless device could potentially provide a means to execute arbitrary code on the BlackBerry Attachment Service component of the BlackBerry Enterprise Server. Vulnerable Systems: BlackBerry Enterprise Server for IBM Lotus Domino version 2.2 and above; BlackBerry Enterprise Server for Microsoft Exchange version 3.6 and above; BlackBerry Enterprise Server for Novell GroupWise version 4.0 and above. Vendor Status: Depending on your environment and the BlackBerry Enterprise Server version, install the appropriate software upgrades.

Refer to source for further solution details.

Source: <http://www.securiteam.com/securitynews/5PP0E0UHPE.html>

- 33. February 14, U.S. Computer Emergency Readiness Team — US-CERT Technical Cyber Security Alert TA06-045A: Microsoft Windows, Windows Media Player, and Internet Explorer vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Windows, Windows Media Player, and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Systems affected: Microsoft Windows; Microsoft Windows Media Player; and Microsoft Internet Explorer.

Further information is available in the following US-CERT Vulnerability Notes:

VU#312956 — Microsoft WMF memory corruption vulnerability:

<http://www.kb.cert.org/vuls/id/312956>

VU#291396 — Microsoft Windows Media Player vulnerable to buffer overflow in bitmap processing routine: <http://www.kb.cert.org/vuls/id/291396>

VU#692060 — Microsoft Windows Media Player plug-in buffer overflow:

<http://www.kb.cert.org/vuls/id/692060>

VU#839284 — Microsoft Windows TCP/IP fails to properly validate IGMP packets:

<http://www.kb.cert.org/vuls/id/839284>

Solution: Microsoft has provided the updates for these vulnerabilities in the Security Bulletins and on the Microsoft Update site.

Microsoft Security Bulletins: <http://www.microsoft.com/technet/security/bulletin/ms06-feb.msp>

Microsoft Update site: <https://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?ln=en&returnurl=https://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us>

Source: <http://www.uscert.gov/cas/techalerts/TA06-045A.html>

- 34. February 13, Security Focus — Hitachi Business Logic multiple input validation vulnerabilities.** Hitachi Business Logic Container is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input. Analysis: Cross site scripting and SQL injection vulnerabilities were found. A malicious remote user can exploit these vulnerabilities to execute invalid scripts and execute arbitrary SQL commands. Vulnerable products: Hitachi Business Logic — Container 03-00-/B; Hitachi Business Logic — Container 03-00; Hitachi Business Logic — Container 02-03. A more detailed list of vulnerable products is contained in this advisory. Solution: The vendor has released advisory HS06-002, along with fixes to address this issue. Please see the referenced advisory for further information on obtaining fixes.

Hitachi Advisory HS06-002: [http://www.hitachi-support.com/security\\_e/vuls\\_e/HS06-002\\_e/](http://www.hitachi-support.com/security_e/vuls_e/HS06-002_e/)



[index-e.html](#)

Source: <http://www.securityfocus.com/bid/16602/references>

35. *February 13, Security Focus* — **Adobe Acrobat and Adobe Reader remote buffer overflow vulnerability.** Adobe Acrobat and Adobe Reader are affected by a remote buffer overflow vulnerability. Analysis: Adobe has discovered a buffer overflow in Adobe Acrobat and Adobe Reader. This issue has been addressed and a product update is available to proactively mitigate potential malicious activity. Affected products: A full list of vulnerable products is contained in this advisory.

Solution: Gentoo Linux has released security advisory GLSA 200508-11 addressing this issue.

For further solution details: <http://www.securityfocus.com/bid/14603/solution>

Source: <http://www.securityfocus.com/bid/14603/discuss>

36. *February 13, Computer World* — **FBI probes hacking incident at Indiana clinic.** A Fort Wayne, IN-based orthopedics clinic with more than a dozen facilities in the state has called in the Federal Bureau of Investigations to investigate a hacking incident that highlights the dangers companies can face from the placement of hidden back doors in their software. The case involves Orthopaedics Northeast, which last month suddenly began experiencing serious performance slowdowns with Webchart, a clinical document management system supplied to the clinic by Medical Informatics Engineering Inc. (MIE). The performance problems, which on one occasion caused the Webchart software to become totally inaccessible for several days, were eventually traced to deliberate changes made in the system's underlying MySQL database, according to Todd Plesko, CEO of triPractix LLC, a medical systems integrator that now manages the clinic's IT services. The database changes were made by someone who illegally accessed the system nine times over a period of two weeks, initially via a back door using a hard-coded username and password, said Plesko. Uncovering the intrusion led to the discovery of "a backdoor realm called MIE Private, with a username of MIE, that would completely bypass all of Webchart's front-end authentication," he explained.

Source: <http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,108639,00.html?SKC=cybercrime-108639>

37. *February 13, VNUNet* — **FTC gets heavy with adware vendors.** The U.S. Federal Trade Commission (FTC) is threatening publicly to humiliate companies if they continue to advertise using ad-serving software. FTC commissioner Jon Liebowitz said at an event hosted by the Anti-Spyware Coalition that the move would aid the fight against adware that tracks users online and displays unwanted pop-up ads. "I think that this could have a beneficial effect," he said. "In this context, maybe shaming a company on how they are spending money might benefit consumer privacy." Liebowitz also suggested publicly shaming advertisers to the other FTC commissioners if the adware issue does not subside.

Source: <http://www.vnunet.com/vnunet/news/2150211/ftc-adware-shaming-naming>

## Internet Alert Dashboard

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of publicly available exploit code for a memory corruption vulnerability in the Mozilla Firefox web browser and Thunderbird mail client. If JavaScript is enabled in these applications, then the system is vulnerable to exploitation. A vulnerable system may be successfully exploited if a user is convinced to visit a specially crafted web page or open a specially crafted email.

A remote, unauthenticated attacker may be able to execute arbitrary code on a compromised system. If the user has elevated privileges, then the attacker will be able to exploit them. For more information please review the following US-CERT Vulnerability Note:

VU#759273 – Mozilla QueryInterface memory corruption vulnerability at URL: <http://www.kb.cert.org/vuls/id/759273>

US-CERT urges users and administrators to implement the following recommendations:

See update to Firefox 1.5.0.1 at URL: <http://www.mozilla.com/firefox/>

Please see SeaMonkey 1.0. at URL: <http://www.mozilla.org/projects/seamoney/>

Disable JavaScript in Thunderbird and Mozilla Suite.

#### Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 25 (smtp), 139 (netbios-ssn), 80 (www), 135 (epmap), 18551 (---), 54000 (---), 6999 (iatp-normalpri) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[[Return to top](#)]

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:  
<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.